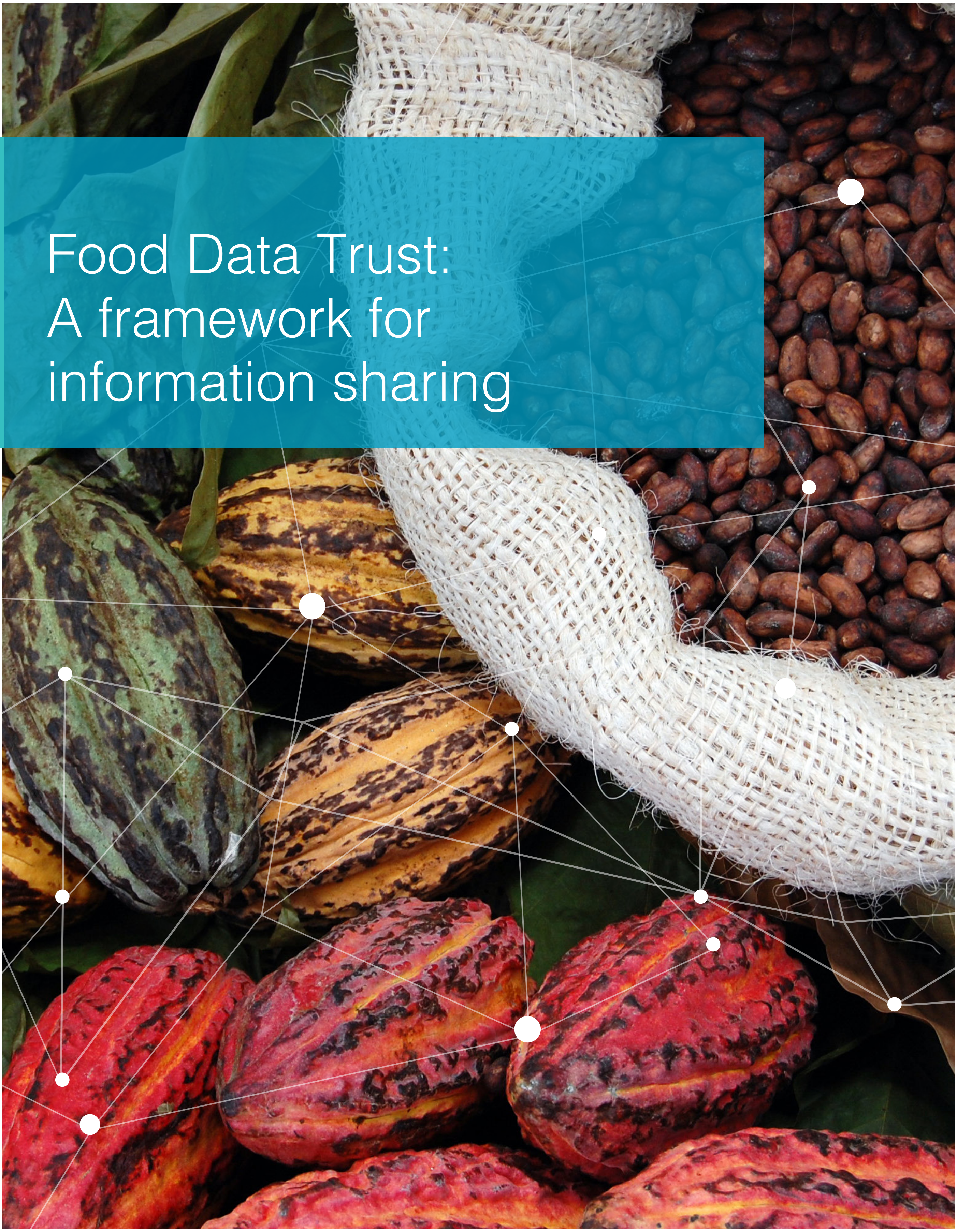
UNIVERSITY OF LINCOLN

Food Standards Agency
food.gov.uk

Food Data Trust: A framework for information sharing



Executive summary

This report examines the role of information sharing in ensuring safe food production supply networks and proposes a data trust framework that will enable efficient and secure data sharing for the benefit of all stakeholders in the food system.

The opportunity

Our food system is evolving in the context of a range of digital opportunities. The potential of automated and autonomous systems, such as fruit-picking robots and smart production lines, of digital technologies such as the Internet of Things and artificial intelligence is becoming ever more evident. We see this not only in 'business as usual' operations but also improved system resilience and robustness. New technologies can also contribute to better outcomes to challenges such as the climate crisis, diet and nutrition issues, antimicrobial resistance and zoonotic diseases.

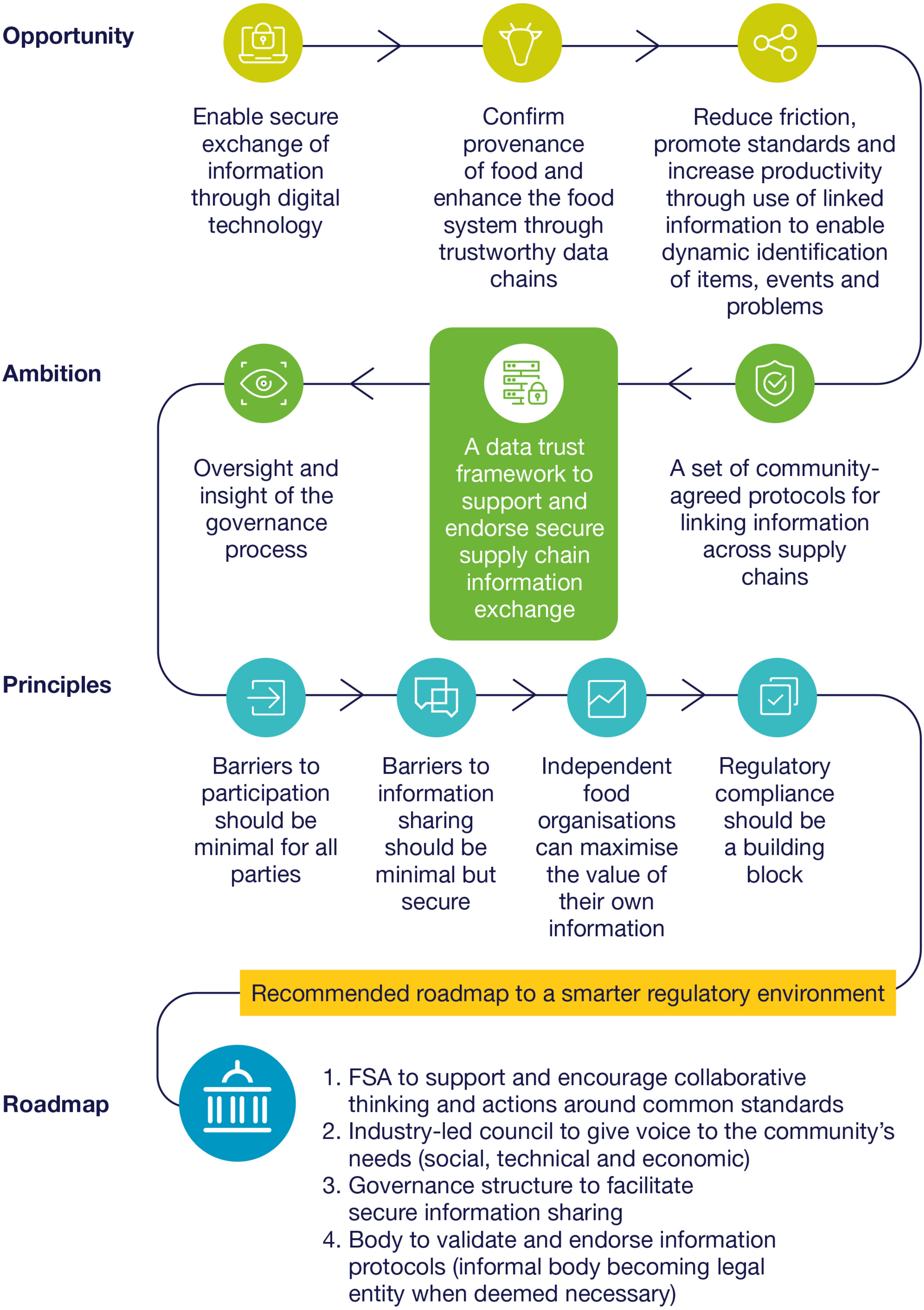
Innovation in the food system can enable new mechanisms to monitor and measure, and therefore support and influence, food standards. Reliable information from across the sector about, for example, allergen data, product authenticity, provenance, nutrition and sustainability, will help serve public needs and and consumer expectations. For food suppliers, it could speed up processes and save money. For the Food Standards Agency (FSA) and the UK government, a move towards easier data sharing could enable a more targeted, risk-based approach to inspections. It could also speed up information exchange along a chain in urgent situations such as food recalls and tracing incidents.

The challenge

It has become far easier to capture and associate information along the food supply chain. However, it can also be a cumbersome process requiring point-to-point data sharing agreements. Sharing information successfully at greater scale will require trust in the quality of the information that is passed along the chain and, critically, trust in the organisations that are sharing it. Evaluating the trustworthiness of this information, and building up trust in the people and organisations involved, takes time and can be complex.

It is clear from our engagement across the food system that while data is certainly playing an increasingly important role in new business models and innovative supply chains, the accessibility and potential use of the data is constrained. Some of these constraints are legislative, such as the 1998 Competition Act which limits the collusive sharing of information, and there are also structural barriers such as insufficient technology standards. Cumulatively, these factors have a detrimental effect how information flows through the supply chain. This data illiquidity means that opportunities are being missed. A significant constraint is rooted in practice and culture: the question of trust.

The vision for information sharing in the food system



Opportunity

Enable secure exchange of information through digital technology

Confirm provenance of food and enhance the food system through trustworthy data chains

Reduce friction, promote standards and increase productivity through use of linked information to enable dynamic identification of items, events and problems

Ambition

A set of community-agreed protocols for linking information across supply chains

A data trust framework to support and endorse secure supply chain information exchange

Oversight and insight of the governance process

Principles

Barriers to participation should be minimal for all parties

Barriers to information sharing should be minimal but secure

Independent food organisations can maximise the value of their own information

Regulatory compliance should be a building block

Recommended roadmap to a smarter regulatory environment

Roadmap

1. FSA to support and encourage collaborative thinking and actions around common standards
2. Industry-led council to give voice to the community's needs (social, technical and economic)
3. Governance structure to facilitate secure information sharing
4. Body to validate and endorse information protocols (informal body becoming legal entity when deemed necessary)

Introduction

Food business operators, regulators and other organisations increasingly seek to use the information captured at various points along the food supply chain more effectively to address a variety of shared objectives. The benefits of such exchanges range from efficiency gains and waste reduction at a transactional level to sector-level opportunities for supply chain optimisation, traceability, resilience and safety. There is now an opportunity for the Food Standards Agency (FSA) and industry to facilitate, and benefit from, more productive and responsible information sharing in the food and drink sector.

How do independent, competing but cooperating organisations choose to make information accessible to each other in a way that is safe, legally valid and demonstrably beneficial? How can building the trust necessary for such exchange be made swifter and simpler?

Data trusts, and more specifically trust frameworks, offer a mechanism to manage decentralised and distributed collections of data that are temporarily linked in limited and specific ways, so that information can be shared securely.

This report addresses the question of how the protection and sharing of information pooled from multiple independent sources should be governed in a legal, secure and trust-building way. A data trust approach offers some aspects of what is needed and, more specifically, a trust framework would enable more efficient and effective information sharing among actors within the UK food supply chain.

As digital technologies transform the landscape of food production and enable new businesses and new business models that harness the opportunities offered by data, there is further need to refocus the regulatory lens from analogue to digital information. This will require regulators to adapt and collaborate. In the case of the FSA, this would support its mission to ensure food is safe and authentic, while respecting and securing food business operators’ commercial sensitivities.

Example challenge area: honey

Honey is a high-value commodity and it is important to be able to detect fraudulent practices, which are increasing, such as adding sugars to honey. However, ‘fingerprinting’ the composition of honey is difficult. Nuclear Magnetic Resonance (NMR) is the technology used to compare the molecular profile of a sample ‘honey’ with the NMR database of genuine honeys to establish authenticity. Commercial laboratories around the world are compiling NMR databases for honey but they are confidential and so cannot be independently audited. Laboratories using different databases even produce different results and there are calls for the external validation and scrutiny of NMR honey databases in a way that does not undermine their commercial value.

A trust framework could allow for improved (governed) inter-laboratory comparisons, if a minimal data requirement and standard can be mutually agreed. This would improve representative sample sizes and reliability, and may help improve regulatory confidence in the approach, provided regulators are incorporated as a framework member, with agreed terms of access.

Not only could a trust framework approach provide benefits to honey sampling, it could also offer greater overarching supply chain assurance for honey, with appropriate information potentially shared between a range of interested parties.

The dimensions of trust and trustworthiness

Maintaining a satisfactory food supply involves an element of trust: trust between the collaborating and competing independent organisations in the supply chain, and trust between the consumer and the food system itself. Trust is difficult to quantify, takes time to establish and can evaporate in no time at all. Trust can be measured and analysed by looking at trustworthiness: factors such as shared values, expertise, reputation and reliability, for example.

Building trust in information sharing

Data institutions are organisations whose purpose involves stewarding data on behalf of others. The Open Data Institute has outlined a range of roles that data institutions might play, including holding data on behalf of an organisation or people and sharing it with others who want to use it for a particular purpose; combining or linking data from different sources and providing insights and other services back to those that have contributed data; creating datasets with different levels of openess that others can access, use and share; and developing and maintaining common data infrastructure for a sector or field, such as by registering identifiers or publishing open standards.

Data trusts have been suggested as one type of data institution to aid information exchange in a range of contexts, most notably in the government-backed report Growing the Artificial Intelligence Industry in the UK.

The benefits of AI are dependent on access to large, comprehensive data collections acquired from multiple sources, not to mention the associated skills and expertise to develop and apply the AI responsibly. The report suggests that data trusts – ad hoc collaborative ventures underpinned by a repeatable framework of terms and mechanisms that enables them to 'share data in a fair, safe and equitable way' – can play a central role in supporting this transformational new workforce with the necessary raw data to achieve their aims.

This centralised model for harnessing AI-related benefits from collected, centralised data has clear benefits for certain organisations, such as balancing different – and often conflicting – views and incentives about how data should be shared and who can access it. The model, further developed by the Open Data Institute, has stimulated a broader debate around the issues. It also leaves a number of aspects open for further expansion, which have been picked up in a range of other papers and reports. These have developed the arguments around privacy, security, common good and accountability. Further work is now needed to facilitate such accountable exploitation of secure and private data.

Trust frameworks

Data trusts are generally envisaged as centralised libraries of information where data is to be securely shared for some greater good. That data is put firmly under the responsibility of a stewardship function that has the responsibility of acting in the interest of all parties. This raises multiple ethical and legal challenges, especially if the trust has more than a narrow, focused agreed purpose on which the stewardship can focus. The data trust's stewardship function may be carried out by one or more individuals who make decisions regarding the data in terms of what can be done with it, and to it, on behalf of the owners and stakeholders. It is possible that the information sources in a data trust could be commercial organisations willing to allow both societal and monetary benefits to be derived from suitably anonymised slices of their commercial data holdings. However, for most transactions of a commercial nature between businesses, and the food sector is no exception, security and privacy are paramount.

Decentralised, liquid, mediated information

In a commercial context a decentralised approach is more realistic, with data retained by the owners in their own distributed data stores and mediated by a body that eases the exchange without seeing the data itself. The concept of a trust framework builds on the principles behind the data trust by accepting these commercial realities, focusing on lowering the barriers for secure information exchange and empowering new forms of collaboration. Rather than collating static, passive data collections, trust frameworks allow for the possibility of monitoring and sampling flows of information both within and between organisations.

Open, closed and shared data

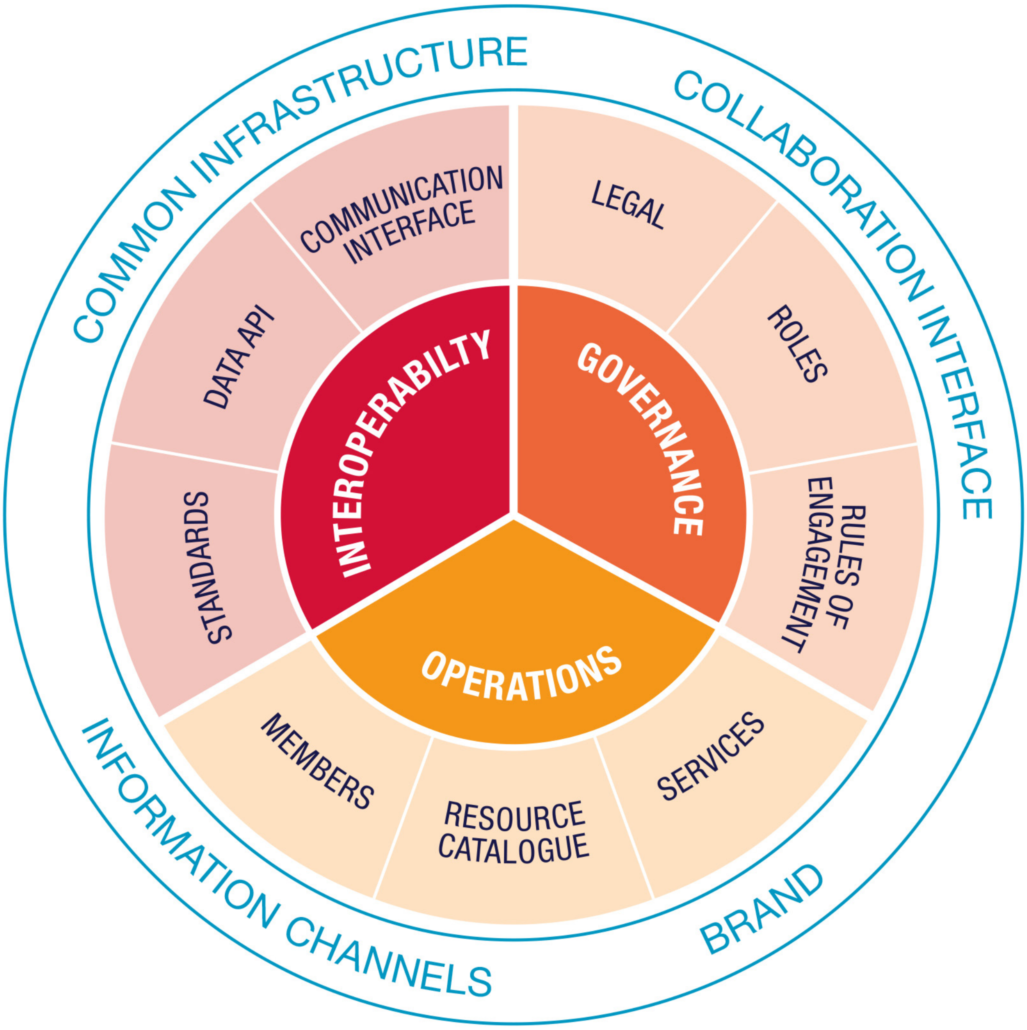
In most organisations data is kept at one or other end of an open/closed data spectrum: either securely closed or else made fully open for public consumption. Controlling access by individuals, roles, groups, data, context etc is tricky because we need to be able to authenticate the identity of individuals and authorise actions. The specific challenge is doing this across separate independent organisations, and with disparate heterogeneous sets of data. FAIR principles, which define findability, accessibility, interoperability and reusability for data may be of help. There are other key characteristics that define data in the context of managed sharing, and these are its liquidity, or preparedness to be shared, and the type of mediation available to handle this sharing. The term liquidity is sometimes used in similar way to the FAIR principles, essentially capturing the need for structure, ideally defined around data format standards, that enable information to be shared and searched. In terms of mediation we are referring to systems that organisations might have access to that transfer information on their behalf that do not have the ability to view the data being transferred.

Defining the boundaries of a data trust for food standards

Our approach to a data trust for food standards is predicated on three pillars of analysis: governance, technology and standards, and business models (contextualised with social, technical, and economic/ legal perspectives). We identified that these three areas would need to be developed and then integrated:

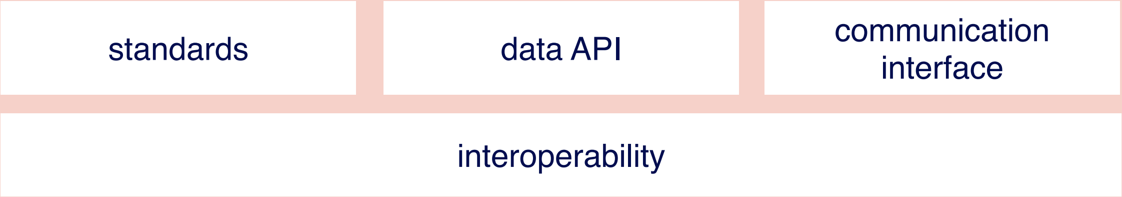
- Governance in terms of the rules and regulations that define interactions.
- Technical standards and mechanisms that enable interoperability between heterogeneous systems.
- The operational structures that deliver the benefits and incentives for the real world.

Conceptual model for the framework



Interoperability

Information sharing requires interoperability between distributed data sources and the systems that manage them. Connecting different information systems is challenging as information is often stored in different formats and housed in different proprietary systems.



standards

data API

communication interface

interoperability

How the community can exchange and share information at a technical level

- Interface for all interactions with the framework.
- Clear and succinct statement of purpose available to all members and non-members, readable by both humans and machines.
- A standards-compliant communication interface, based on user experience principles, enables humans and machines to make simple approaches to the data trust.
- The data API provides interoperability individually with all of the member organisations against pre-defined contractual arrangements (standards compliant and based on FAIR – findable, accessible, interoperable and reusable – principles).

Operations

How the community interacts at a business level

- Directory of members and their roles and organisations may be accessible.
- There is no limit to the number of classes of membership but details must be contained within governance layer.
- Catalogues of data and metadata may be accessible.

Governance

Legal matters and organisational responsibilities needed to ensure the system operates satisfactorily to meet community's needs

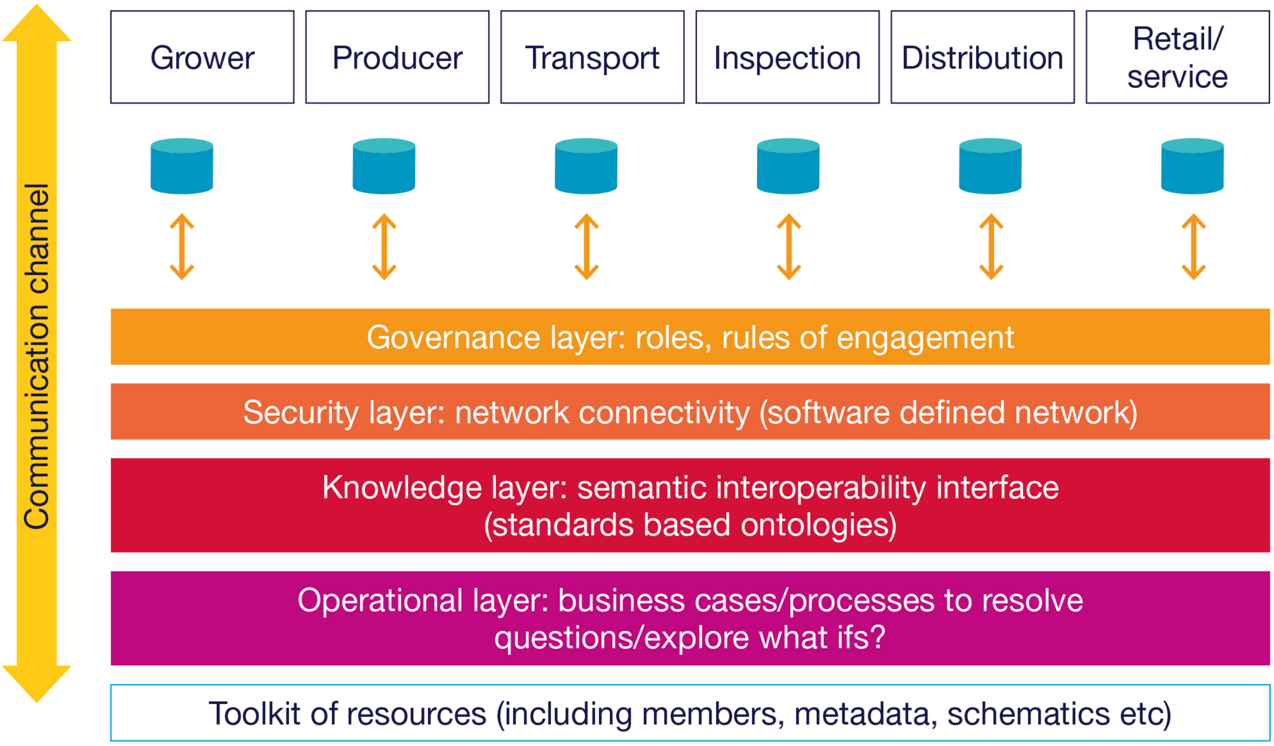
- All the rules and regulations for the framework are contained within the governance layer.
- The legal structure defines the legal terms under which everything within the framework operates, including responsibilities and liabilities. It is the practical guide to what can and cannot be undertaken by the members. All of which ensures that no single partner organisation can take control.
- Rules define the responsibilities, competences and liabilities attached to the various roles members may be assigned.

A key feature of the governance framework is the need for a **legal structure** to define the operating model. We discuss this further, and the legal report associated with this document, in the Legal Framework section on p16.

Implementation of food data trusts / trust frameworks

Trust frameworks are needed to implement extensible and adaptive information sharing structures for distributed food supply networks. There may be multiple ways to achieve this, with a variety of technologies, but we suggest that the following logical layers will be needed for any solution that addresses the principles and requirements that we have identified.

Conceptual model of the logical layers of interaction within a data trust framework



Communication channel
Grower
Producer
Transport
Inspection
Distribution
Retail/ service
Governance layer: roles, rules of engagement
Security layer: network connectivity (software defined network)
Knowledge layer: semantic interoperability interface (standards based ontologies)
Operational layer: business cases/processes to resolve questions/explore what ifs?
Toolkit of resources (including members, metadata, schematics etc)

Management and orchestration

The key characteristic of a data network for a food production supply chain is distributed data stores. These data stores would belong to independent organisations, such as a haulier, retailer and farm, each with responsibility for their own data. Any flows of information corresponding to a flow of goods between these organisations would be controlled in a decentralised manner. Retailers may request information from suppliers but would not typically have free access to all of their data. Similarly, producers would receive selected data from their suppliers, and would pass on or make available selected information to hauliers. For routine transactions, functional and regulatory processes would dictate information flows. Only in exceptional cases, such as product recalls and other incidents, would further protocols around extra data be enacted.

Various technologies exist to enable distributed information stores to be integrated in a suitable way. Software Defined Networking (SDN) separates the hardware – the plumbing – of information networks from the architecture that describes how the pipes are connected together. Separating the management of the network technology from the orchestration of the information flows allows networks to evolve and adapt to the business needs of the collaborating partners. A further degree of security and resilience can be introduced through the concept of Zero Trust Network architecture. This approach is particularly relevant to distributed supply chains where it is not a case of a single organisation managing all of the data in their own walled garden of trust. When zero trust is taken as a starting point, a collection of independent organisations must question and justify every request to share or exchange information. Such an approach has a number of requirements, including a need to have strongly authenticated users, rules and policies for accessing data.

Data sharing in action in banking

Open banking, a series of reforms to how banks deal with and share consumers' financial information, has the potential to revolutionise the banking and fintech ecosystem. Open banking is a collaborative model in which banking data is shared through an API (application programming interface - a documented set of connecting points that allow an application to interact with another system) between two or more unaffiliated parties to deliver enhanced capabilities to the marketplace. The potential benefits of open banking include improved customer experience, new revenue streams and a sustainable service model for traditionally underserved markets.

Communication protocol

A further challenge for integrating information across a distributed food supply chain is that the independent organisations will each have their own collections of information systems, their own data architectures and their own vocabularies or metadata schemas to describe their data. The word tomatoes may refer to individual fruits, bunches of vine tomatoes, tins of San Marzano plum tomatoes, or crates of tomatoes. The challenge is to enable information to be visible from different points in the chain. In order to coordinate actions and decisions along the supply chain there must be links between the independent data sets.

One way of forming these links is to make use of semantic web standards and linked data principles. Semantic web standards include Resource Description Framework (RDF), a structured data model for sharing information, and Web Ontology Language (OWL), for representing rich and complex knowledge about things. Considerable work has been done already in applying these technologies to the food system. This includes attempts to map knowledge about the food system in the form of an ontology of linked terms describing foodstuffs and the relationships between them.

More recent work, such as that from the TNO, has addressed the particular challenge of pedigree and traceability requirements. The challenge is to establish the wider trust mechanisms that would validate the information along the chain.

The benefit of these semantic technologies is that we can address the need to develop fragments of ontologies that can be created around specific scenarios and dynamically map supply chains to specific incidents and challenges. More detailed and comprehensive work has been undertaken in this vein by the Open Ecosystem Federation (OEF) project led by a coalition of government departments, including HMRC, Future Borders and Food Standards Agency, which has been developing a technical toolkit and governance models. The underlying governance mechanism is based on legal principles of a data trust.

Open Ecosystem Federation (OEF)

A service that enables a technology-agnostic toolkit to support collaboration between people, organisations, and machines in a way that is scalable, repeatable, and extensible.

The governance model

If a decentralised and independent food system that is dependent on secure flows of information is to flourish, a degree of alignment will be needed to coordinate the standards and other protocols that dictate how data is shared and exchanged. This could best be achieved through a robust coordinating mechanism that brings together the collaborating parties from across the food system, including regulators and other legally empowered gatekeepers, to agree the necessary protocols.

We propose a two-tier governance structure that enables relevant stakeholders to participate in and learn from the process. We have examined a range of successful ventures at national level in similar domains, including banking and freight.

Data sharing in action in logistics

The Dutch data sharing initiative iSHARE is a government-supported collaboration that helps the Dutch transport and logistics sector improve its efficiency, reducing costs and carbon dioxide emissions through connecting different stakeholders with a trust framework. For example, before iSHARE's launch in 2018, the Dutch logistics sector was inefficient due to road congestion. Trucks were waiting in harbours, unclear if the ship they needed was already in the harbour or the specific location of their container. The ship and container data was inaccessible, fragmented and difficult to share between partners. Planning could not be optimised and the supply chain remained inefficient.

Through a uniform set of identification, authentication and authorisation agreements that enable organisations in the transport and logistics sector to share data effortlessly, iSHARE has made it possible for the sector to:

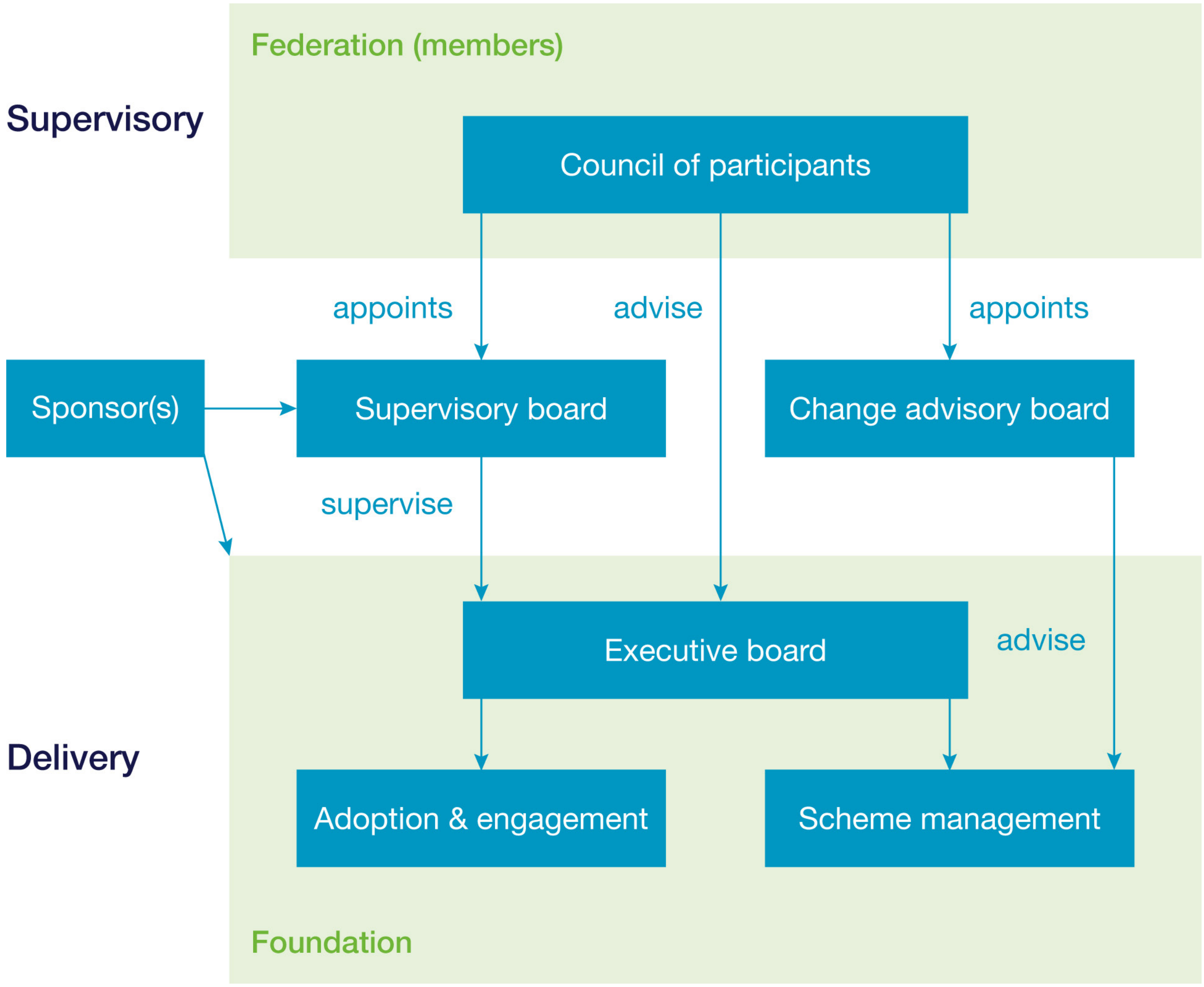
- Avoid costly and time-consuming integrations in order to share data.
- Share data with new and previously unknown partners.
- Maintain full control over its own data at all times. It has the final say about the terms under which its data will be shared, why, with whom and for how long.

The iSHARE Foundation, as the governing data institute, plays a crucial role. By signing up with the Foundation, logistics enterprises can join the network of organisations that all operate in line with the iSHARE Agreements. The iSHARE Foundation works independently, transparently and not for profit.

There are three components of our proposed two-tiered governance structure. The members' council that comprises representatives of all stakeholders concerned with data trust frameworks, a supervisory board elected by that council that can represent the council and determine priorities, and hence supervise an executive board that is tasked to focus on the day-to-day strategies for developing and implementing the data trust framework protocols such as identity, authentication and authorisation mechanisms.

In the short and medium term this could be achieved through a collection of adaptable collaboration agreements based around those that have been developed in a series of recent projects. Ultimately, it may be beneficial to establish a legal entity to represent this two-tier governance structure.

Two-tier governance structure



The legal framework

The scalability of any data-sharing solution will depend upon a trustworthy framework being in place to underpin that sharing. The trust that a robust and reliable framework is capable of engendering among its participants will reduce the need for every participant to trust each other participant on an individual basis.

Pinsent Masons has produced a legal report examining possible contractual and corporate models for data sharing. There are key elements that are common to all these structures, however, and that we believe are essential to engendering trust among stakeholders.

These are:

- A clear statement of purpose, underpinned by robust governance.
- Transparent and consistent decision-making.
- Accountability between stakeholders.

While the benefits of data sharing can be manifold, stakeholders will want to know that any data to which they provide access will be used for appropriate and ethical purposes. Strong governance can achieve this.

The legal report looks at various models of governance, many of which comprise some form of stakeholder membership body – often broad in nature – and a smaller decision-making body. Subject matter expert committees (such as in respect of ethics and technology) can report into or advise that decision-making body. However simple or complex the preferred governance model may be, the fact that the decision-making process is both transparent and consistent will reassure stakeholders that their data is being dealt with in an appropriate manner.

Beyond that, if any stakeholder breaches the terms of the framework, the other stakeholders will want to know that appropriate sanctions are available against that stakeholder. Most obviously this might take the form of access to the courts or arbitration to determine disputes or enforce rights, but it might also, at some point in the future, include access to a regulator who could be responsible for enforcing a code of conduct.

The full legal report and this report are available on the FSA website and at the following DOIs: 10.5281/zenodo.4575565 (this report) and 10.5281/zenodo.4575625 (the legal report).

The way forward

The food production supply system is increasingly dependent on the secure sharing and exchange of information among independent organisations and official regulators. The efficiency of this sharing and exchange of information could have a significant influence on how successful our food system becomes in the future. We believe that there is a unique opportunity right now in terms of the availability of new technologies and the challenges of a regulated food industry to optimise these processes.

Towards an intelligent food chain

The goal that we envisage is an intelligent, decentralised food supply chain driven by the secure exchange and sharing of information. This can range from secure passing of regulatory compliance information to unique insights derived from artificial intelligence harnessing the accumulative benefits of secure collections of distributed data.

Achieving this goal requires robust and resilient data-driven services, secure and independent AI services accessing anonymised independent data, and a firmly human-centred governance representing all stakeholders in the food system, including the consumer. There are already several initiatives implementing data exchange mechanisms between food sector businesses. These do not universally propose a common set of objectives. In our roadmap, regulatory compliance can and should be better enabled by data trust frameworks and contribute to a more resilient and robust food chain. Our roadmap also aims to improve the visibility and discussion of data trust frameworks across a wider cross-section of food sector players. We aim to bring together insights from various sources in a technologically agnostic forum.

The legal report that accompanies this report describes in more detail the issues surrounding establishment of the necessary collaboration agreements that provide the backbone to a data trust.

Data sharing in action: BlueRing

The BlueRing platform enables organisations to share information between their own business-critical legacy systems. The platform acts as a secure broker and buffer between new and/or less trusted providers, such as cloud services, but also the geographical constraints such as poor bandwidth often found in the areas of the world where the produce sector is situated.

We suggest that a small-scale trial would provide further insight into these ideas. This could complement projects such as the BlueRing trial being undertaken as part of the Innovate UK-funded Trusted Bytes project. This could take the form of the Food Data Trust (FDT) described in the companion legal report. This should be undertaken in conjunction with relevant regulators and with the participation of commercial bodies as well as academic support. Industry engagement will be essential; the mechanism should be co-designed and co-developed with industry partners relevant to each use case.

Roadmap

There are several interdependencies in the development of the Food Data Trust. The Internet of Food Things (UK-wide EPSRC-funded multi-disciplinary research network for digitalised food system) is well-placed to support this.

The proposed next steps for delivery of the FDT are:

1. Establish a representative Advisory Group (Council) drawn from across the sector in order to provide support to the steering committee at a strategic level

2. Establish a Steering Committee to lead technical oversight of an FDT pilot structure, and, if deemed appropriate, help create the legal entity

3. Form a Communications Hub to gather and disseminate information and knowledge in relation to trusted data exchanges and opportunities this can unlock

4. Deploy a data trust virtual observatory to collect and analyse evidence on the operation and effectiveness of the FDT pilot

Principles

We see a roadmap to a food data trust composed of many related initiatives in the form of smaller projects (case studies) that will develop and demonstrate the different elements of the data sharing protocol. These will range from the Innovate UK-funded Trusted Bytes project (funded to address some of these issues in the context of trans-national trade in food products) to smaller pilot studies such as those directly supported by partners including the FSA. From our investigations the following principles have emerged.

These should underpin the implementation of our recommended actions.

Principles

Any mechanism as a minimum should ensure that:

1. Barriers to entry for cooperating partners are as low as possible

2. Information flows can be optimised in order to lower barriers for information sharing

3. It maximises the value of data, through reuse, repurpose, and validation

4. It aids compliance with regulatory obligations

5. Data is retained within and by the owning organisation: your data is your data

6. Work activity should not be duplicated if at all possible

7. Core codes of practice (protocols, set of agreements) are contained in a collaboratively agreed common playbook

References

Alves, H. (2013) ‘Co-creation and innovation in public services’, **Service Industries Journal,** 33(7–8), pp. 671–682. doi: 10.1080/02642069.2013.740468.

Brewster, C. et al. (2020) ‘Ontology-based Access Control for FAIR Data’, **Data Intelligence,** 2(1–2), pp. 66–77. doi: 10.1162/dint_a_00029.

Delacroix, S. and Lawrence, N. D. (2019) ‘Bottom-up data Trusts: Disturbing the “one size fits all” approach to data governance’, **International Data Privacy Law**, 9(4), pp. 236–252. doi: 10.1093/idpl/ipz014.

Dutch Government (2019) **Dutch vision on data sharing between businesses**.

Edwards, L. (2004) ‘Reconstructing consumer privacy protection on-line: a modest proposal’, **International Review of Law, Computers & Technology**, 18(3), pp. 313–344. doi: 10.1080/1360086042000276762.

Ganin, A. A. et al. (2020) ‘Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management’, **Risk Analysis**, 40(1), pp. 183–199. doi: 10.1111/risa.12891.

Gorwa, R. (2019) ‘What is platform governance?’, **Information Communication and Society**. Taylor & Francis, 22(6), pp. 854–871. doi: 10.1080/1369118X.2019.1573914.

Hall, W. and Pesenti, J. (2017) **Growing the Artificial Intelligence Industry in the UK.**

Hammerstein, M. (Barclays) and Starks, G. (ODI) (2015) **The Open Banking Standard.**

iSHARE: Sharing Dutch transport and logistics data (no date) Support Centre for Data Sharingta Sharing.

Kansas State University (2020) ‘Feed the Future innovation lab for collaborative research on sustainable intensification’, (September).

Kronthal-Sacco, R. et al. (2019) ‘Sustainable Purchasing Patterns and Consumer Responsiveness to Sustainability Marketing’, **SSRN Electronic Journal**. doi: 10.2139/ssrn.3465669.

Li, W. et al. (2014) ‘Integrated clinical pathway management for medical quality improvement - Based on a semiotically inspired systems architecture’, **European Journal of Information Systems**, 23(4), pp. 400–417. doi: 10.1057/ejis.2013.9.
Martindale, W. et al. (2020) ‘Testing the data platforms required for the 21st century food system using an industry ecosystem approach’, **Science**

of the Total Environment. Elsevier B.V., 724, p. 137871. doi: 10.1016/j.scitotenv.2020.137871.

Miying Yang, Palie Smart, Mukesh Kumar, M. J. & S. E. (2018) ‘Product-service systems business models for circular supply chains’, **Production Planning & Control The Management of Operations**. doi: 10.1080/09537287.2018.1449247.

Mothershaw, N. (OIX) (2020) OIX Guide to Trust Frameworks.

Murphy, H., Warrell, H. and Sevastopulo, D. (2020) ‘The great hack attack: SolarWinds breach exposes big gaps in cyber security I Financial Times’, **Financial Times**, pp. 1–10.

ODI (2019) **Data trusts: lessons from three pilots (report).**

Pearson, S. et al. (2019) ‘Are Distributed Ledger Technologies the panacea for food traceability?’, **Global Food Security**, 20. doi: 10.1016/j.gfs.2019.02.002.

Schmitt, B. (2019) ‘From Atoms to Bits and Back: A Research Curation on Digital Technology and Agenda for Future Research’, **Journal of Consumer Research,** 46(4), pp. 825–832. doi: 10.1093/jcr/ucz038.

Sharing, G. R., Data, O. and Report, P. (2020) **Mechanisms to Govern Responsible Sharing of Open Data_ A Progress Report.**

Solanki, M. and Brewster, C. (2013) ‘Consuming linked data in supply chains: Enabling data visibility via linked pedigrees’, **CEUR Workshop Proceedings**, 1034.

Song, M. et al. (2017) ‘How would big data support societal development and environmental sustainability? Insights and practices’, **Journal of Cleaner Production**. Elsevier Ltd, 142, pp. 489–500. doi: 10.1016/j.jclepro.2016.10.091.

Stalla-Bourdillon, S., Wintour, A. and Carmichael, L. (2019) **Building Trust Through Data Foundations A Call for a Data Governance Model to Support Trustworthy Data Sharing.**

Strange, N. (2020) **In a time of uncertainty, Bank of England.**

Wilkinson M D (2016) The FAIR Guiding Principles for scientific data management and stewardship. Sci Data. 2016 Mar 15;3:160018. doi: 10.1038/sdata.2016.18

Wolff, J. (Blavatnik School of Government, U. of O. (2018) ‘Risk and the Regulation of New Technologies’, p. 23.

Zhang, X. et al. (2020) ‘A 2020 research commentary on the trust repair life cycle for “How to use apology and compensation to repair competence- versus integrity-based trust violations in e-commerce.”’, **Electronic Commerce Research and Applications.** Elsevier, 40(January), p. 100945. doi: 10.1016/j.elerap.2020.100945.

About this report

This report was commissioned by the Food Standards Agency (FSA, project ref FS301083). This report is based on use cases involving field work, interviews, desk-based investigation and analysis from existing research. It builds on the work of the Internet of Food Things Network+ (EPSRC project grant number: EP/R045127/1) in the area of digital collaboration, in particular research work on Digital collaboration in the food and drink production supply chain.

This report was written by:
- Professor Simon Pearson, University of Lincoln
- Steve Brewer, University of Lincoln
- Dr Philip Godsiff, University of Exeter
- Prof Roger Maull, University of Exeter

With support from:
- Prof Jeremy Frey, University of Southampton
- Prof Gerard Parr, University of East Anglia
- Prof Andrea Zisman, Open University
- Prof Luc Bidaut, University of Lincoln

We would like to thank everyone who has contributed time and insights to this report through interviews, discussions and working groups. We have drawn on their knowledge and experience but, of course, this report does not necessarily reflect or endorse the views or policy positions of any of the individuals listed below. Thank you to:

- Food Standards Agency
- Suffolk Coastal Port Health Authority
- Barfoots
- GS1
- Internet of Food Things Network+ (IoFT)
- IoFT working groups for Ethics and Data Sharing
- Office for AI
- Open Data Institute
- Alan Ainsworth, Open Banking Entity
- Sarah Cameron, Pinsent Masons LLP
- Sam Cannicott and Lawrence Kay, Centre for Data Ethics and Innovation
- Claire Chapman, Office for AI
- Dr Christopher Brewster, TNO
- Martin Collison, Collison and Associates
- Peter Crocker, Oxford Semantic Technologies
- Peter Crosskey, food industry specialist
- Nick Davies, HMRC
- Dr Matthew Dovey, Jisc

- Ben Goodall, FSA
- Philip Griffiths, NetFoundary
- Eefje van der Harst, Innopay, NL
- Tom Hollands, Raynor Foods Ltd
- Stefan Janusz, Office for AI
- Sid Kalita, FSA
- Dr Samantha Kanza, University of Southampton
- Dr Wouter Los, University of Amsterdam
- Dr Wayne Martindale, National Centre for Food Manufacturing
- Andrew McMillan, Pinsent Masons LLP
- Gareth Roberts - Regather, Sheffield
- Ben Sheridan, BSI
- Richard Stirling (Oxford Insights), Open Data Institute (ODI))
- Prof Mark Swainson, National Centre for Food Manufacturing
- Alex Szymborski, Contained Technologies UK
- Justin Szymborski, Fesa UK Ltd
- Dr Sian Thomas, Department of International Trade
- Dr Mying Yang, University of Exeter

Editorial support: Michelle Pauli
Project management: Infoculture
Design: Stoats & Weasels

Contact details

Steve Brewer
sbrewer@lincoln.ac.uk
University of Lincoln

Sid Kalita
Sid.kalita@food.gov.uk
Food Standards Agency

Report created March 2021

DOI: 10.5281/zenodo.4575565